



FortiAnalyzer Upgrade Guide

VERSION 5.2.1

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com

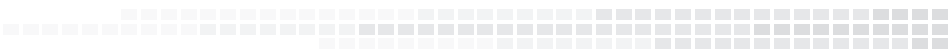


December 12, 2014

FortiAnalyzer 5.2.1 Upgrade Guide

05-521-256032-20141212

TABLE OF CONTENTS



- Change Log** **4**
- FortiAnalyzer Firmware** **5**
 - Best practices 5
 - Firmware image naming convention 6
 - FortiAnalyzer VM firmware 6
 - SNMP MIB download 7
 - Build numbers 7
 - Firmware upgrade and support information 7
- Upgrade Information** **12**
 - Upgrading from FortiAnalyzer v5.2.012
 - Upgrading from FortiAnalyzer v5.0.8 or v5.0.912
 - Firmware upgrade steps12
 - Distributed upgrades14
 - Downgrading to previous versions14

Change Log

Date	Change Description
2014-12-12	Initial release.

FortiAnalyzer Firmware

This document provides an overview of FortiAnalyzer firmware and highlights general information you should be aware of prior to upgrading your device. This guide is intended to supplement the *FortiAnalyzer Release Notes* documentation.

The following topics are included in this section:

- [Best practices](#)
- [Firmware image naming convention](#)
- [FortiAnalyzer VM firmware](#)
- [SNMP MIB download](#)
- [Build numbers](#)
- [Firmware upgrade and support information](#)

Best practices

- Before any firmware upgrade complete the following:
- Download the firmware image and Release Notes document from the [Fortinet Customer Service & Support](#) portal. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Prepare your device for upgrade and ensure your log devices are running the appropriate firmware versions as documented in the firmware Release Notes.
- Backup your configuration file and save this configuration file to your local computer. The device configuration file is saved with a `.dat` extension.



In VM environments, it is recommended that you clone the VM instance. In the event of an issue with the firmware upgrade, you can revert to the VM clone.



In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider.

-
- Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or log devices.
 - Once the upgrade is complete, test your device to ensure that the upgrade was successful and that all log devices are listed.



Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiAnalyzer Release Notes* or contact Fortinet Technical Support.



Upgrading the device firmware can trigger an SQL database rebuild. During this time, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status. The following features will not be available until after the SQL database rebuild has completed: FortiView, Log View, Event Management, and Reports.

Firmware image naming convention

Firmware images in the [Fortinet Customer Service & Support](#) portal HTTPS and FTP Download tabs are organized by firmware version, major release, and patch release. The firmware images in the folders follow a specific naming convention and each firmware image is specific to the device model. For example, the FAZ_300D-v500-build0618-FORTINET.out image found in the `/FortiAnalyzer/v5.00/5.2/5.2.0` file folder is specific to the FortiAnalyzer 300D device model.

FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for both VMware ESX/ESXi and Microsoft Hyper-V Server virtualization environments.

Microsoft Hyper-V Server

- FAZ_VM64_HV-v500-buildxxxx-FORTINET.out: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- FAZ_VM64_HV-v500-buildxxxx-FORTINET.out.hyperv.zip: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

- FAZ_VMxx-v500-buildxxxx-FORTINET.out: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- FAZ_VMxx-v500-buildxxxx-FORTINET.out.ovf.zip: Download either the 32-bit or 64-bit package for new FortiAnalyzer VM installations. The package contains a deployable Open Virtualization Format (OVF) virtual machine package for VMware ESX/ESXi installations and the faz.vmdk and datadrive.vmdk virtual machine disk format files.

For more information see the FortiAnalyzer product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortianalyzer/virtualappliances.html>.

SNMP MIB download

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main version 5.00 file folder.

Build numbers

Firmware images are generally documented as a three-digit build number. New models may be released on a branch based off of the regular firmware release. As such, the build number found in the *System Settings > Dashboard, System Information* widget and the output from the `get system status` CLI command displays this four-digit build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point:` field that displays the regular three-digit build number.

Firmware upgrade and support information

The following table is for reference only. Review the applicable *FortiAnalyzer Releases Notes* prior to upgrading your device.

Upgrade and support information

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.2.1	0662	5.2.0 5.0.8, 5.0.9	5.2.0, 5.2.1, 5.2.2 5.0.0 to 5.0.10 4.3.2 to 4.3.18
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
5.2.0	0618	5.0.6, 5.0.7, 5.0.8, 5.0.9	5.2.0, 5.2.1 5.0.0 to 5.0.9 4.3.2 to 4.3.18
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
5.0.9	0345	5.0.7, 5.0.8	5.2.0, 5.2.1 5.0.0 to 5.0.10 4.3.2 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			

Upgrade and support information

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.0.8	0335	5.0.7	5.2.0, 5.2.1 5.0.0 to 5.0.9 4.3.2 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
5.0.7	0321	5.0.6	5.2.0 5.0.0 to 5.0.9 4.3.2 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
FAZ-3900E is released on build 4053.			
5.0.6	0310	5.0.5 4.3.7 or later	5.0.0 to 5.0.7 4.3.2 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
FAZ-3000E is released on build 4047.			
FAZ-3500E is released on build 4031.			
5.0.5	0266	5.0.4 4.3.7	5.0.0 to 5.0.4 4.3.2 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
5.0.4	0232	5.0.3	5.0.0 to 5.0.4 4.3.2 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
5.0.3	0200	5.0.1 or 5.0.2	5.0.0 to 5.0.3 4.3.2 to 4.3.18 4.2.0 to 4.2.15

Upgrade and support information

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV. FAZ-VM64-HV is released on build 0200. FAZ-1000D is released on build 4024.			
5.0.2	0151	5.0.1	5.0.0 to 5.0.2 4.3.2 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. FAZ-300D is released on build 4018. FAZ-3000D is released on build 4014.			
5.0.1	0087	4.3.5 or later	5.0.0 and 5.0.1 4.3.1 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. FAZ-300D is released on build 4008.			
5.0.0	0076	This image was removed from the Customer Service & Support portal. For more information, see the <i>Customer Support Bulletin</i> in the image directory.	
4.3.8	0719	4.3.5 or later 4.2.6	4.3.0 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.7	0705	4.3.5 or later 4.2.6	4.3.0 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.6	0691	4.3.5 4.2.6	4.3.0 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.5	0680	4.3.3 or later 4.2.6	4.3.0 to 4.3.18 4.2.0 to 4.2.15

Upgrade and support information

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
Supported models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
There is no image available for the FAZ-200D.			
4.3.4	0679	4.3.3 4.2.6	4.3.0 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
There is no image available for the FAZ-200D.			
4.3.3	0654	4.3.2 4.2.6	4.3.0 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
FAZ-200D is released on build 4010.			
4.3.2	0632	4.3.1 4.2.5 or later	4.3.0 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
FAZ-400C is released on build 4006.			
4.3.1	0552	4.3.0 4.2.4 or later	4.3.0 to 4.3.18 4.2.0 to 4.2.15
Supported models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, and FAZ-VM.			
4.3.0	0513	4.2.4 or later	4.3.0 to 4.3.18
Supported models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, and FAZ-4000B.			
There is no image available for the FAZ-VM.			



Upon upgrading to version 5.0.1 or later, the system automatically begins converting the version 4.3 logs, and inserts them into the SQL database. An icon appears at the top right corner after login to the Web-based Manager next to the logout and help buttons. This pops-up a small window displaying the progress. The time required depends on the size of the database.



Upgrading a FortiAnalyzer VM device from version 4.3.6 or later to version 5.0.1 or later is supported. The old VM license is converted into the new VM stackable license model. New VM installations running version 5.0.1 or later can be deployed with the `.ovf` (VMware ESX/ESXi) or `.vhd` (Microsoft Hyper-V) file and application of either an old version 4.3 or new version 5.0 license.

Upgrade Information

This section explains how to properly upgrade to FortiAnalyzer 5.2.1. The following topics are included in this section:

- [Upgrading from FortiAnalyzer v5.2.0](#)
- [Upgrading from FortiAnalyzer v5.0.8 or v5.0.9](#)
- [Firmware upgrade steps](#)
- [Distributed upgrades](#)
- [Downgrading to previous versions](#)

Upgrading from FortiAnalyzer v5.2.0

FortiAnalyzer 5.2.1 supports upgrade from v5.2.0.

Upgrading from FortiAnalyzer v5.0.8 or v5.0.9

FortiAnalyzer 5.2.1 supports upgrade from v5.0.8 or v5.0.9.

Firmware upgrade steps

The following table lists the firmware upgrade steps.

Upgrade steps

Step 1	Prepare your device for upgrade.
Step 2	Backup your system configuration.
Step 3	Transfer the firmware image to your device.
Step 4	Log into the Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your device for upgrade

1. Make sure all log devices are running the supported firmware version as stated in the Release Notes.
2. Log in to the Fortinet Customer Service & Support portal at <https://support.fortinet.com>.
3. Select *Download* from the toolbar and select *Firmware Images* from the drop-down list.
4. Select *FortiAnalyzer* from the drop-down list and select the *HTTPS Download* tab. Alternatively, you can select *FTP Download*. FTP is not an encrypted file transferring protocol and HTTPS download is recommended.
5. The image folders are displayed.
6. Browse to the appropriate file folder to download the firmware image (.out) and Release Notes document.
7. Select an image in the list to download the firmware image to your management computer.

8. To verify the integrity of the download, select *Download* from the toolbar and select *Firmware Image Checksums* from the drop-down list.
9. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Back up your system configuration

1. Go to *System Settings > Dashboard*.
2. Select *Backup* in the *System Information* widget. The *Backup* dialog box opens.
3. Select the checkbox to encrypt the backup file and enter a password.
4. Select *OK* and save the backup file on your local computer.



When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the device..

Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:



```
execute backup all-settings {ftp | sftp} <server IP address>  
<path/filename to the server> <user name on server> <password>  
[cryptpasswd]
```

```
execute backup all-settings scp <server IP address> <path/filename to  
the server> <user name on server> <SSH certificate> <crptpassrd>
```

For more information, see the [FortiAnalyzer CLI Reference](#).

Step 3: Transfer the firmware image to your device

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*. The *Firmware Upgrade* dialog box opens.
3. Select *Browse* to locate the firmware image (.out file) that you downloaded from the [Fortinet Customer Service & Support](#) portal and select *Open*.
4. Select *OK* to continue with the upgrade. Your FortiAnalyzer will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.



Optionally, you can upgrade firmware stored on a FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path on the FTP server>  
<server IP address <user name on server> <password>
```

For more information, see the [FortiAnalyzer CLI Reference](#).

Step 4: Log into the Web-based Manager to verify the upgrade was successful

1. Refresh the browser page and log back into the device.
2. Launch the *Device Manager* module and make sure that all formerly added log devices are still listed.

3. Launch the other functional modules and make sure they work properly.

Distributed upgrades

For Collector/Analyzer architecture upgrades, Fortinet recommends upgrading the Analyzer first.



Upgrading the Collector first could impact the Analyzer's performance.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the Web-based Manager or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```



High Performance Network Security



Copyright© (Undefined variable: FortinetVariables.CopyrightYear) Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.